АДМИНИСТРАЦИЯ МУНИЦИПАЛЬНОГО РАЙОНА «НЕРЧИНСКИЙ РАЙОН» ЗАБАЙКАЛЬСКОГО КРАЯ

РАСПОРЯЖЕНИЕ

25 марта 2020 г. № 156

г. Нерчинск

Об утверждении Положения об учете, хранении и использовании носителей ключевой информации, криптографических средств и электронной подписи в администрации муниципального района «Нерчинский район»

В целях исполнения требований Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи», Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»:

1. Утвердить Положение об учете, хранении и использовании носителей ключевой информации, криптографических средств и электронной подписи в администрации муниципального района «Нерчинский район» (приложение);

2. Контроль над исполнением настоящего распоряжения возложить на заместителя руководителя администрации муниципального района «Нерчинский район» по территориальному развитию (Бутин А.Н.).

Глава муниципального района
«Нерчинский район» Р.В. Сенотрусов

Приложение
к распоряжению администрации
муниципального района «Нерчинский район»
от «25» марта 2020 г. № 156

Положение об учете, хранении и использовании носителей ключевой информации, криптографических средств и электронной подписи в администрации муниципального района «Нерчинский район»

1. Общие положения

1. Настоящее положение разработано в соответствии с Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи», Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

2. В положении использованы следующие термины и определения:

Администратор безопасности информации - лицо, организующее, обеспечивающее и контролирующее выполнение требований безопасности информации при осуществлении обмена электронными документами.

Электронная цифровая подпись (ЭЦП) - реквизит электронного документа, предназначенный для защиты данного электронного документа от подделки, полученный в результате криптографического преобразования информации и позволяющий идентифицировать владельца ключа, а также установить отсутствие искажения информации в электронном документе.

Средства криптографической защиты информации (далее - СКЗИ) и квалифицированная электронная цифровая подпись предназначены для подписания электронных документов ЭЦП с целью подтверждения подлинности информации, ее авторства и шифрования при передаче по открытым каналам связи для обеспечения конфиденциальности.

Закрытый ключ подписи - уникальная последовательность символов, известная владельцу сертификата и предназначенная для создания в электронных документах электронной цифровой подписи с использованием средств ЭЦП.

Открытый ключ подписи - уникальная последовательность символов, соответствующая закрытому ключу подписи, доступная любому пользователю информационной системы и предназначенная для подтверждения подлинности ЭЦП в электронном документе.

Сертификат ключа подписи (сертификат) - документ на бумажном носителе или электронный документ, который включает в себя открытый ключ ЭЦП и который выдается удостоверяющим центром для подтверждения подлинности ЭЦП и идентификации владельца сертификата.

Носитель ключевой информации (ключевой носитель) - материальный носитель информации, содержащий закрытый ключ подписи или шифрования.

Шифрование - способ защиты информации от несанкционированного доступа за счет ее обратимого преобразования с использованием одного или нескольких ключей.

2. Порядок работы с СКЗИ и средствами ЭЦП

3. СКЗИ и средства ЭЦП могут использоваться для защиты конфиденциальной информации, не содержащей сведений, составляющих государственную тайну.

4. Электронная цифровая подпись выдается на один год с момента изготовления. Срок действия ЭЦП указан в сертификате. По истечении этого срока владельцу ЭЦП необходимо провести плановую смену ЭЦП в Удостоверяющем центре.

5. Использование ЭЦП определяется администратором безопасности информации в соответствии с распоряжение администрации муниципального «Нерчинский район» о разрешении использования ЭЦП в конкретной информационной системе (программе).

6. ЭЦП является аналогом собственноручной подписи и должна использоваться только ее владельцем в соответствии с ограничениями, содержащимися в сертификате. Пользователь принимает на себя риски, связанные с неправомочным использованием ЭЦП и средств ЭЦП, с подделкой, подлогом либо иным искажением информации, которая содержится в документах, предоставленных Пользователем для получения ЭЦП, компрометацией используемых ключей ЭЦП, нарушений Регламента оказания услуг Удостоверяющего центра.

7. Для работы с СКЗИ и средствами ЭЦП в качестве пользователя привлекаются уполномоченные лица от администрации муниципального «Нерчинский район», назначенные соответствующим распоряжением администрации муниципального «Нерчинский район».

8. Работу с ключами ЭЦП и шифрования координирует администратор безопасности информации.

9. Должностные лица, уполномоченные соответствующим распоряжением администрации муниципального «Нерчинский район», могут эксплуатировать СКЗИ, получать и использовать ключи шифрования и ЭЦП, несут персональную ответственность за:

- сохранение в тайне конфиденциальной информации, ставшей им известной в процессе работы с СКЗИ;
- сохранение в тайне содержания закрытых ключей ЭЦП;
- сохранность носителей ключевой информации.

10. Для исключения возможности доступа к ЭЦП посторонних лиц, несанкционированного использования или копирования ключевой информации должны быть обеспечены условия хранения ключевых носителей. Для обеспечения безопасности ЭЦП Пользователя, необходимо:

- хранить ключи ЭЦП на специальных защищенных носителях - электронных идентификаторах с использованием надежного пароля.
- обеспечить надежное хранение носителей ключевой информации, исключающее доступ к ним посторонних лиц, не передавать сами носители лицам, к ним не допущенным;
- вставлять ключевой носитель при проведении работ, не являющихся штатными процедурами использования ключей (шифрование/расшифровывание информации, проверка электронной цифровой подписи и т.д.);
- не записывать на ключевой носитель постороннюю информацию;

не вносить какие-либо изменения в программное обеспечение СКЗИ и средств ЭЦП;

- не использовать бывшие в работе ключевые носители для записи новой информации без предварительного уничтожения на них ключевой информации путем переформатирования.

3. Проверка электронной цифровой подписи

11. Для создания и проверки электронной цифровой подписи используются средства ЭЦП, которые:

-позволяют установить факт изменения подписанного электронного документа после момента его подписания;

- обеспечивают практическую невозможность вычисления ключа электронной подписи из электронной подписи или из ключа ее проверки.

12. При проверке электронной цифровой подписи средства ЭЦП должны:

-показывать содержимое электронного документа, подписанного электронной подписью;

- показывать информацию о внесении изменений в подписанный электронной подписью электронный документ;

- указывать на лицо, с использованием ключа электронной подписи которого подписаны электронные документы.

13. Пользователь может осуществлять проверку ЭЦП как с помощью используемых средств ЭЦП, так и обратившись в Удостоверяющий центр. Процедура проверки ЭЦП в электронном документе в Удостоверяющем центре описана в Регламенте оказания услуг Удостоверяющего центра.

4. Уничтожение ключевой информации

14. После прекращения действия ключей ЭЦП они должны быть удалены с ключевого носителя и проведена замена ключей и сертификатов ключей.

15. Плановая смена ключей и сертификатов открытых ключей осуществляется ответственным лицом администрации муниципального «Нерчинский район» за месяц до окончания срока их действия.

16. Внеплановая замена ключей и сертификатов закрытых ключей проводится в следующих случаях:

- компрометация ключей;

- изменение идентификационных данных и/или областей использования ключа, указанных в заявлении на изготовление ключей;

5. Выход из строя ключевого носителя

17. К событиям, относящимся к компрометации ключей, относятся следующие ситуации:

- утрата ключевых носителей ключа;

- утрата носителей ключа с последующим обнаружением;

- увольнение сотрудников, имевших доступ к ключевой информации;

- возникновение подозрений на утечку информации или ее искажение в системе конфиденциальной связи;

- нарушение целостности печатей на сейфах с носителями ключевой информации, если используется процедура опечатывания сейфов;

- утрата ключей от сейфов в момент нахождения в них носителей ключевой информации;

- утрата ключей от сейфов в момент нахождения в них носителей ключевой информации с последующим обнаружением;

- доступ посторонних лиц к ключевой информации.

Пользователь самостоятельно должен определить факт компрометации закрытого ключа и оценить значение этого события для Пользователя.

Мероприятия по розыску и локализации последствий компрометации конфиденциальной информации, переданной с использованием СКЗИ, организует и осуществляет администрация муниципального «Нерчинский район».

При компрометации ключа администратор безопасности администрации муниципального «Нерчинский район» должен немедленно поставить в известность Удостоверяющий центр о факте компрометации ключей, сообщив номер сертификата. В течение 30 минут после поступления сообщения о компрометации ключа, действие его будет приостановлено до подачи в Удостоверяющий центр письменного заявления об аннулировании скомпрометированных ключей.

Возобновление работы с ЭЦП будет возможно только после замены скомпрометированных ключей.

6. Эксплуатация и хранение электронного идентификатора (носителя ЭЦП)

18. Рекомендуется хранить ключевые носители в помещениях, которые имеют прочные входные двери с установленными на них надежными замками. В обязательном порядке для хранения ключевых носителей в помещении должно использоваться металлическое хранилище (сейф, шкаф, секция) заводского изготовления, оборудованное приспособлением для его опечатывания.

19. Транспортирование ключевых носителей за пределы организации допускается только в случаях, связанных с производственной необходимостью. Транспортирование ключевых носителей должно осуществляться способом, исключающим их утрату, подмену или порчу.

20. На технических средствах, оснащенных средствами ЭЦП, должно использоваться только лицензионное программное обеспечение фирм-производителей.

21. Запрещается оставлять без контроля вычислительные средства, на которых эксплуатируется ЭЦП после ввода ключевой информации. При уходе пользователя с рабочего места должно использоваться автоматическое включение парольной заставки.

22. Ключевая информация содержит сведения конфиденциального характера, хранится на учтенных в установленном порядке носителях и не подлежит передаче третьим лицам.

23. Ответственный исполнитель ЭЦП обязан вести журнал учета хранения электронных носителей конфиденциальной информации и своевременно заполнять его (приложение 1).

24. Закрытые ключи изготавливаются в 2-х экземплярах: эталонная и рабочая копии. В повседневной работе используется рабочая копия ключевого носителя.

25. При физической порче рабочей копии ключевого носителя, пользователь немедленно уведомляет об этом администратора безопасности администрации муниципального «Нерчинский район».

26. Категорически не допускается:

- осуществлять несанкционированное копирование ключевых носителей;
- разглашать содержимое ключевых носителей и передачу самих носителей лицам, к ним не допущенным, а также выводить ключевую информацию на дисплей и принтер;
- использовать ключевые носители в режимах, не предусмотренных правилами пользования ЭЦП, либо использовать ключевые носители на посторонних ПЭВМ;
- записывать на ключевые носители постороннюю информацию.

27. Для нормальной работы носителя ЭЦП, необходимо придерживаться следующих правил эксплуатации и хранения:

1) Не разбирать электронный идентификатор, это ведет к потере гарантии! Кроме того, при этом возможна поломка корпуса электронного идентификатора, поломка элементов печатного монтажа и т. д.

2) Оберегать электронный идентификатор от механических воздействий (падения, сотрясения, вибрации и т. п.), воздействия высоких и низких температур, агрессивных сред, высокого напряжения.

3) Не прилагать излишних усилий при подсоединении электронного идентификатора к порту компьютера.

4) Не допускать попадания на электронный идентификатор (особенно на его разъем) пыли, грязи, влаги и т. п. При засорении разъема электронного идентификатора принять меры для его очистки. Для очистки корпуса и разъема использовать сухую ткань. Использование органических растворителей недопустимо.

5) В случае неисправности или неправильного функционирования электронного идентификатора обращаться в Удостоверяющий центр.

Приложение

ФОРМА

Журнал учета хранения электронных носителей конфиденциальной информации

№ записи	№ ключа	ФИО сотрудника получившего ключ	Обоснование для использования ключа	Дата использования ключа		Подпись сотрудника
				Время получения	Время возврата	